Primary Online Safety Framework Document

Manor Beach Primary School

Please use the following two documents to help you to complete and Online Safety Policy for your school.

- The Lancashire Online Safety Framework Document (this document)
- The Lancashire Online Safety Guidance Document

What are the two documents for?

The Lancashire Online Safety Guidance Document offers support and prompts to enable you to consider the appropriate responses to Online Safety in your school and is intended to be used alongside the Online Safety Framework.

The Online Safety Framework Document enables you to collate your responses from the Guidance Document into the appropriate sections. Once completed, the Online Safety Framework Document will present a clear picture of how your school responds to Online Safety providing you with an Online Safety policy for your school.

Your completed Online Safety Policy would form part of the Lancashire Online Safety Charter.
For further information about the Lancashire Online Safety Charter please see http://www.lancsngfl.ac.uk/OnlineSafety

How to use the Lancashire Online Safety Framework Document (this document)

- Refer to the Lancashire Online Safety Guidance Document as a prompt for discussion.
- Complete each section of this document (Online Safety Framework) to reflect your school context.
- The sections in italics are to help you to structure the content of your policy and can be deleted as appropriate.
- The sections in bold text are intended to provide a starting point to develop your school's responses.
- The completed document will provide you with your school's Online Safety policy.

Developing and Reviewing this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people:

.....

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: ……

The implementation of this policy will be monitored by ……..

This policy will be reviewed as appropriate by ……..

Approved by …… (Headteacher) Date ……

Approved by …… (Governor) Date ……

Contents

Online Safety Policy 2018 Manor Beach Primary School

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Vision for Online Safety

Manor Beach Primary School aims to provide a diverse, balanced and relevant approach to the use of technology where the children have the opportunity to learn in an environment where security measures are balanced appropriately in order for children to be able to learn effectively. We aim to equip the children with the skills and knowledge to use technology appropriately and raise awareness of the risks of technology both inside and outside the school community. We feel it is essential that children have strategies to deal with these risks. As a school we recognise the need for an effective e safety policy.

3. The role of the school's Online Safety Champion

The Online Safety Champion for Manor Beach Primary School – Andrew Brown

Our Online Safety Champion is Andrew Brown

The role of the Online Safety Champion in our school includes:

- To have operational responsibility for ensuring the development, maintenance and review of the schools Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensure that the policy is implemented and that compliance with the policy is actively monitored.
- Ensure all staff are aware of reporting procedures and requirements should an

Online Safety incident occur.

- Ensure the Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary. Liaising closely with the school's Designated Senior Person for E safety (H Davies) / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and practices

This Online Safety policy should be read in conjunction with the following other related policies and documents:

Child Protection
Mobile Phone Policy
ICT Policy
EVC Policy

4.1 Security and data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:
Accurate
Secure
Fairly and lawfully processed
Processed for limited purposes
Processed in accordance with the data subject's rights
Adequate, relevant and not excessive
Kept no longer than is necessary
Only transferred to others with adequate protection.

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

Within school there are 2 different networks – admin and curriculum.
Admin network

- Password protected at the appropriate level for the necessary members of staff to access.
- Passwords regularly changed

- Within access to the computer programs password protected again at the most appropriate level to the seniority of the staff.
- Data transferred securely to other schools.

Curriculum network

- Curriculum computers managed by a domain server which is password protected.
- All staff have individual log ins to access the computer which allow access only to their personal folder and folders with shared access.
- Class log in which enable children to save in their class folder but prevent children from changing settings within control panel.
- Administrator log in – Access by technician and ICT SL only.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

School Laptops need to be signed for when allocated to a member of staff and returned to school when the member of staff leaves/changes position.

- All school laptops will be set up in the same way by the ICT Technician.
- Any software required by the member of staff will be installed by the ICT SL or technician.
- No other additional software should be installed unless permission is given by ICT SL.
- Any problems/errors with a laptop and it should be returned to school and reported to ICT SL.
- Laptops are configured to work with standard routers or phone lines. (Any alteration to settings needed must be carried out by the school technician and this could incur a charge to the individual member of staff.)
- Laptops may not be used for personal access to Social Networking, Chat Rooms or instant messaging. Only recognised educational bulletin boards or public discussion groups should be used e.g. TES
- Use of laptops at home follow the same conditions as internet usage in school.

Cameras

To protect all staff no personal cameras or cameras on mobile phones should be used in school or on educational visits to take photos of children. All pictures on school cameras should be downloaded onto the school network.

School laptops/ tablets

Any digital equipment must be signed out in a book kept in the office and the rules above apply

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- The school seeks consent from parents/carers as to whether their child may appear in the media. A list of children whose photo must not appear on the school website is circulated among staff.
- Parental/Carers permission is obtained.
- Images of pupils have they have left the establishment may be kept on the school server but are not used in any publications beyond a year after they have left.
- Staff are aware that full names and personal details will not be used in any digital media and particularly in association with photographs.
- Parents and Carers are allowed to take photographs/videos at events as long as there is no objection from other parents and carers attending. It is asked that they are not published on social media
- It is made clear to all staff that photographs and videos are only taken using school equipment, the children are appropriately dressed and then are only downloaded onto the school network where only authorised users can log on and access.
- Parents and Carers are directed to online safety sites where the dangers of publishing images and videos of pupils or adults on social network or websites without the consent of the person involved is clearly explained.

4.4 Communication technologies

In our school the following statements reflect our practice in the use of email.

Email:

The government encourages the use of e-mail as an essential means of communication. Direct e-mails can bring significant educational benefits however the following points need to be addressed.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must tell a teacher immediately if they receive offensive e-mails.
- Pupils must not reveal details of themselves or others, such as address or telephone number or arrange to meet anyone in e-mail communication.
- Pupils must use an appropriate tone and language when sending e-mails.
- Whole class e-mails should be used at KS2, KS1 and Foundation.
- Pupils will not be allowed to access public or unregulated chat rooms.
- Children will only use regulated chat environments when supervised by an adult and chat room safety will be emphasised. E.g. Kidsmart to teach children about chat room safety.

- Pupils are **not allowed** to access personal e-mail using school Internet facilities, due to the quantity of unsolicited e-mail (Spam), unsuitable content and virus threats associated with commercial e-mail accounts.
- The school will use Office 365 as its email service in school

Staff

- All users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.
- Only official email addresses should be used to contact staff/pupils.
- The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

The Lancashire E-mail include a standard disclaimer at the bottom of all outgoing emails (see example below).

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Manor Beach Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks: Need to consider access to Twitter on admin

These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools therefore staff and children are unable to access through the school network.

The DCSF document 'Guidance for Safer Working Practice for Adults who work with **Children and Young People (available to view**

http://webarchive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resources-and-practice/ig00311/

Lancashire County Council Guidance relating to the use of social networking sites is as follows:

Where information can easily reach a wider audience than might have originally be intended, in certain circumstances, the conduct of the employee might also be deemed to have damaged the reputation of the school and the trust and confidence in the school that parents and the community can reasonably expect.

Therefore the authority's advice to staff is that they should be very careful in how they communicate with pupils via the use of technology and in terms of what they elect to share about themselves through internet based networking sites such as Facebook and Twitter.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

The main points being

- Staff should not give their personal contact details to children or young people, including their mobile number, details of any blogs or personal website.
- Internet or web based communication channels should not be used to send personal messages to a child/young person.
- Social networking sites are not to be used by children or adults within school. Ensure that if a social networking site is used outside of the workplace, details are not shared with children and young people and privacy settings are set at maximum.
- Laptop and other handheld devices which are borrowed or loaned out to members of staff should not be used to access social networking sites for a personal nature.
- Inappropriate comments about the work place are not posted
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- Pupils must not be added as "friends" on any Social Network site.
- Twitter may be accessed on the Admin network and must only accessed by Headteacher, DSL for online safety or the ICT subject leader

Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Staff may use ClassDojo as a means of sharing and communicating information with parents. This function is only to be used by staff in school. No pictures of children should be shared and messages should be kept professional. If picture(s) of children's work is shared, staff should ensure that the work is anonymous to protect the child and his/her identity.

Mobile

Mobile telephone:

Mobile phone use and ownership by young people is growing. Manor Beach does not permit children to have mobiles in school without written permission and they should be switched off at all times and left in the school office. The following risks are made clear to pupils when using mobiles outside of school

- Exposure to inappropriate material
- Physical danger
- Cyberbullying
- Legal, financial and commercial considerations (ref Becta Signposts to safety)

Staff are made aware of the risks of unfiltered internet content when accessing through a mobile phone and the apps which can access personal details on phones.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

Staff

- Keep personal phone numbers private and personal mobile phones should not be given to parents. Personal mobiles should not be used to contact pupils or parents, except in an emergency when the mobile number needs to be withheld.

- When on a school trip if a contact number is needed for parents this should be a school mobile not a teacher's personal mobile.

-Mobiles to be on silent during teaching sessions and only use them at break times or with permission from the Head Teacher

-Pictures not to be taken of children using personal mobile phones.

Instant Messaging:

In our school, the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

- The use of Instant messaging (e.g. MSN messenger) is not permitted
- Use of social-networking websites (e.g. Twitter, MySpace, Facebook, Instagram, Piczo, etc.) is not permitted.
- Children and staff must not access public or unregulated chat rooms.
- Children may access web based games/activities (Sumdog , Bug club, SPag.com, Mymaths). This may involve playing against users from other schools but should not extend to communication with other users

Instant Messaging is only appropriate in school when part of a Video Conferencing session through CLEO where images are transmitted through a webcam through a secure link.

Sexting

Sexting can be defined as the activity of sending text messages that are about sex or intended to sexually excite someone. This is not appropriate for school and any instance of this between children will be treated as an online safety/child protection incident and will be dealt with by the Online Safety Ambassador and Child Protection Lead in school.

The school policy on instant messaging and social networking prohibits this in any case (see above).

Web sites and other online publications

Content of School Website

Publication of information on a website should be considered from a security point of view.

- The point of content on the web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will only be used if parents have given permission
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- The website should be subject to frequent checks to ensure that no material has been inadvertently posted, which may put children or staff at risk.
- Copyright and intellectual property rights must be respected
- When photographs to be used on the website are saved, names of individuals should not be used as file names.

Importance of the Internet and benefits to education.

- The purpose of the Internet is to raise educational standards to promote pupil achievement, to support professional work of staff and to enhance the schools management information and business administration system.
- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils world-wide.
- Staff professional development through access to national developments educational material and good curriculum practice.

Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

Staff and pupils are not allowed to **download** programs from the Internet or via e-mail programs such as Hotmail onto school computers without permission from the ICT SL /Technical support officer

Emerging technologies will be examined for educational benefit and downloaded if they are seen to be appropriate for educational use by the ICT SL or technician

Video conferencing:
Video Conferencing is a valuable tool bringing the outside world into the classroom.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- Parents' carers will have signed a consent form enabling their child to participate in video conferencing sessions.
- Headteacher to approve video conferencing sessions. All session times should be logged including the date, time and name of the external organisations taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'stop' or 'hang up' the call.
- Copyright, privacy and Intellectual property Rights IPR legislation will be breached if images, video or sound are recorded without permission.
- Check whether recordings are repurposed in any other form or media other than the purpose originally agreed.

4.5 Acceptable Use Policy (AUP)

Your school needs a number of Acceptable Use Policies (AUPs) to ensure that all users stay safe whilst using the internet and other communication technologies. These policies MUST reflect the technologies, procedures and practice within individual schools. For more information and examples of various AUPs see section 4.5 (Acceptable use policy [AUP]) and related Appendices in the Lancashire Online Safety Guidance Document.

4.6 Dealing with incidents

An incident log (see Appendix 10) will need to be completed to record and monitor offences. This must be audited on a regular basis by the Online Safety Champion and the Headteacher.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). **Never personally investigate, interfere with or share evidence as you may**

inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident

(See Appendix 11). Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) .They are licensed to investigate – schools are not!
Examples of illegal offences are:
Accessing child sexual abuse images
Accessing non-photographic child sexual abuse images
Accessing criminally obscene adult content
Incitement to racial hatred
More details regarding these categories can be found on the IWF website
http://www.iwf.org.uk

Online Safety Incidents

- The ICT SL, Online Safety Champion, and the headteacher are responsible for dealing with Online Safety incidents.
- All staff are aware of the types of Online Safety incidents and how to respond appropriately. E.g. illegal or inappropriate
- Chart – see appendix outlines procedures in place to deal with E Safety incidents.
- Children are informed of procedures during Online Safety sessions
- Incidents are logged – see appendix
- Incidents are logged by one of the named people dealing with the incident (ICT SL, e-Champion, Headteacher)
- Appropriate measures are put in place to respond to incidents and prevent a recurrence of an incident.
- Parents and external agencies are informed as appropriate (see appendices)

5. Infrastructure and technology -

Manor Beach Primary School subscribes to Bt Lancashire Education Service. Lightspeed provides internet content filtering. The filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti Virus software is included in the schools subscription and is installed on all computers and configured to receive regular updates. Any virus alerts are e-mailed to bursar@manorbeach.lancs.sch.uk

Pupil Access:

Pupils log on to the network using their class user name and password.

Pupils are supervised when using the internet or other online materials.

Passwords:

- Staff are aware of the guidelines in the Lancashire ICT Security Framework
- All users of the school network have a secure username and password. The level of access and permission is appropriate to their status.

- The administrator password is known by the ICT SL, E champion and school technician. A copy is kept in an envelope in the school safe.
- Through online safety lessons children are reminded of the importance of keeping passwords secure.
- Children's passwords are changed annually. Office admin network passwords are changed every _____

Software/hardware:

- Manor Beach has legal ownership of all software.
- Software is appropriately licenced and a file of licences are kept in the ICT store room
- Equipment and software is audited. Equipment is recorded in the school stockbook. All staff have a list of software on computers.
- ICT SL and technician controls what software is installed on the schools systems.
- Manor Beach have purchased and manage licenses for the software used online.

Managing the network and technical support:

- Servers, wireless systems and cabling is securely located and physical access is restricted.
- All wireless devices go through the schools proxy server
- Wireless devices are only accessible through a secure password
- ICT SL with the support of the ICT technician is responsible for managing the security of the school network.
- Safety and Security of the school network is reviewed annually or more frequently if issues occur. Group policies are distributed from the server to keep children safe.
- Computers and laptops are kept up to date with updates and patches rolled out from the server. The ICT Technician periodically ensures updates have taken place.
- Staff and pupils are required to log or lock out of a computer when left unattended.
- Only the administrator is allowed to download executable files or install software.
- Breaches or security or suspicion of breaches of security are reported to the ICT SL and recorded in folder in office.
- Removable storage devices may be used by school staff and visitors as long as they use SOPHOS to scan device before opening folders.

- External technical support providers are aware of the schools requirements and standards regarding e safety.
- ICT SL/E Safety Champion is responsible for liaising with Technical support staff.

Filtering and virus protection:

- Staff report websites which need blocking or unblocking to ICT SL
- Staff report suspected or actual computer virus to ICT SL
- School laptops automatically update antivirus protection when connected to the internet.

6. Education and Training

6.1Online Safety across the curriculum

Acceptable access to the Internet.

It is necessary to develop good practice when accessing the Internet and develop it as a tool for teaching and learning. The quantity of information needs to be cut down by guiding pupils to appropriate web sites rather than suggesting use of the whole Web.

- The school Internet access will be filtered with a service known as Smart Filter.
- Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.
- Children will be taught the principles of effective searching as part of their core digital literacy skills development.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Planned unit of Online Safety is taught in each year group and linked to other subjects where appropriate. Within this children are made aware of the relevant legislation when using the internet (appropriate to age group) e.g. data protection Act 1998 and copyright implications. Children are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.
- This unit also covers cyberbullying and the impact it can have. PSHE is used to address any issues throughout the year and children are provided with strategies and points of contact if they need help.
- There is an additional focus on E Safety during the National Online Safety Awareness Week
- Online Safety education is differentiated for pupils with SEN by using the most appropriate materials to meet their needs.
- Children are taught to critically evaluate materials and sources of information on the internet so research skills can be used effectively across the curriculum.

- Children are taught about the need to stay safe at school and how to stay responsible outside school. Pupils are reminded of these rules through displays in the ICT room, e safety rules which are sent home and Online Safety guidelines next to each computer.

6.2Online Safety – Raising staff awareness

- Online Safety Champion/ICT SL has received recent Online Safety training
- All staff are expected to promote and model responsible use of ICT and digital resources.
- The safety policy is discussed with all new staff to ensure they understand the content and the procedures in place.
- Updates on the Online Safety policy are discussed at staff meetings

6.3Online Safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

- School newsletters and website provide information on the benefits and risks of using various technologies.
- School promotes external e safety resources and online materials.
- School uses Twitter to communicate with parents and raise awareness of Online Safety

6.4Online Safety – Raising Governors' awareness

Governors are kept up to date through reports at governor meetings and through a governor with specific responsibilities for ICT.

The Online Safety policy is reviewed by the governing body.

7 Standards and inspection

The children will be knowledgeable about how to stay safe online and understand who to talk/report to if there is a problem. Parents are aware of where to get support and the dangers their children face in a digital world and measures they can put in place to reduce the risks.

E Safety incidents are recorded by staff and monitored by E Safety Champion (A Brown), DSL for Online Safety and Headteacher. Policies and procedures are reviewed in light of any incidents.

Any incidents are recorded are monitored to see if there is any recurring pattern or whether they are a one off.

Staff recognise the importance of staying safe online and model this.

AUP's are reviewed annually with the Online Safety policy reviewed bi annually.

This section of the policy should explain how implementation of your policy will be monitored. For more information, see section 7 (Standards and inspection) in the Lancashire Online Safety Guidance Document.